

## نصائح السلامة:

# حافظوا على أنفسكم وسلامتكم عند استخدام الشبكة العالمية

تولي دائرة الشؤون التربوية والثقافية بوزارة الخارجية الأمريكية بالغ الأهمية لمسائل الأمن والسلامة المتعلقة باستخدامكم لشبكة الإنترنت، ولذلك نرجو أن تتقروا بالنظر في نصائح السلامة التالي ذكرها عند استخدامكم للموقع الشبكي الاجتماعي والبريد الإلكتروني والإنترنت:

1. لا تشرعوا إطلاقاً أية معلومات اتصال شخصية على شبكة الإنترنت، ولا تقوموا في أي وقت بإدراج عنوان البريد الإلكتروني أو رقم الهاتف في أي موقع إلكتروني عام مثل الصفحة التعريفية الخاصة بكم أو في أي مدونة أو منتدى أو تعليق على إحدى صوركم.
2. إذا كنتم تتممرون ببعضوية أحد المواقع الشبكية الاجتماعية، ننصحكم بإعارة انتباهكم مكافف لإعدادات الخصوصية المتعلقة بشخصكم، علماً أن هذه الإعدادات تسمح لكم بتحديد مدى البيانات الشخصية التي يتم الكشف عنها وكذلك بتحديد الجهات التي تستطيع الاطلاع على هذه البيانات.
3. افحصوا بعناية أي شيء تريدون نشره على الموقع الشبكي الاجتماعية. وننصحكم بالامتناع عن نشر أي صورة أو فيديو أو نص على هذه الموقع إذا كان اطلاع أحد أفراد عائلتكم أو أحد منسوبين جهه عملكم على مثل هذه المواد سيؤدي إلى نوع من الإحراج لكم.
4. قبل إضافة أي ملحق لربط ملف التعريف الخاص بكم ("الودجة"—أحد التطبيقات للشارك الإلكتروني مع الآخرين)، ننصحكم بالنظر فيما إذا كنتم فعلاً تريدون تمكين الشخص الذي قام بإنشاء هذا الملحق من الوصول إلى الصفحة التعريفية وإلى البيانات الخاصة بأشطافكم في الموقع الشبكي الاجتماعي. ولا تتسرعوا أن الموقع الشبكي الاجتماعي عادة لا تستطيع التحكم في هذه الملحقات، ولذلك ننصحكم بتوكيل الحذر عند استخدام هذا النوع من الأدوات.
5. قوموا بإبلاغ إدارة الموقع الشبكي عن أي انتهاكات لشروط الاستخدام الخاصة بذلك الموقع. وعموماً تتتوفر في كافة المواقع الشبكية الرصينة، بما في ذلك الموقع الاجتماعي منها، وسيلة ما تمكنكم من القيام بالتبليغ عن الانتهاكات.
6. إن البريد الإلكتروني قابل لاستخدامه بغرض نشر البرامج الخبيثة أو للحصول على بياناتكم الشخصية بغية ارتكاب أعمال الاحتيال. ولحماية أنفسكم والحواسيب التي تستخدمونها، نرجو أن تتقروا بمراعاة المبادئ التوجيهية المبينة أدناه:

- يجب توخي بالغ الحذر عند التعامل مع الرسائل الإلكترونية والمكالمات الهاتفية التي تتلقونها دون سابق طلب من أفراد يرغبون في الحصول على بيانات شخصية. وإذا ادعى شخص غير معروف لكم أنه يتبع لهؤوسسة مشروعة، ننصحكم بالسعى للتحقق من هوية ذلك الشخص بصفة مباشرة عند تلك المؤسسة.
- عندما تردون على أية رسائل إلكترونية أو مكالمات هاتفية لم تتطرق من مبادرتكم أنتم، يجب أن تتجنبوا في جميع الأوقات الكشف عن بيانات شخصية أو مالية (مثل أرقام بطاقات الائتمان والرقم السري الخاص ورقم التعریف).
- لا تقوموا بإرسال أية بيانات شخصية أو مالية عبر الانترنت قبل التحقق من الوضعية الأمنية للموقع الشبكي المعنى. (تبدأ عناوين المواقع الشبكية الآمنة دائمًا بعبارة: "<https://>").
  - افحصوا عنوانين المواقع الشبكية الموجودة في أعلى الشاشة دائمًا بعناية. وقد تبدو المواقع الشبكية الخبيثة تماماً مثل الموقع الأصلي المشروع، إلا أن العنوان قد يستخدم ترکيبة أحرف مختلفة أو نطاقاً بديلاً (مثل: ".com" بدلاً من: ".net").
  - قوموا بتوفير الحماية الازمة لحواسيبكم وسائر الحواسيب الأخرى التي تستخدمنها، وذلك عن طريق فحص جميع الوسائل المنقولة مثل محركات فلاش والأقراس الدمجية أو الونقية قبل فتح أي ملفات موجودة في مثل هذه الوسائل، وذلك بغية التتحقق من عدم وجود أية فيروسات داخل هذه الملفات وكذلك عن طريق فحص كافة الملحقات التي تتلقونها عبر البريد الإلكتروني قبل فتح أي من هذه الملحقات.
  - لا تقبلوا أو تفتحوا أية ملفات تنفيذية واردة إليكم عبر البريد الإلكتروني (والمؤشر عليها في نهاية اسم الملف بالأحرف الثلاثة: ".exe")، علماً أن مثل هذه الملفات التنفيذية قد تكون ذات خطورة بالغة.

